**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Call Authentication Trust Anchor | ) | WT Docket No. 17-97 |
| | ) | |

# COMMENTS OF CTIA


Thomas C. Power
Senior Vice President, General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

Melanie K. Tiano
Director, Cybersecurity and Privacy

**CTIA**
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081


August 14, 2017

## TABLE OF CONTENTS

**Before the**
**FEDERAL COMMUNICATIONS COMMISSION**
**Washington, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Call Authentication Trust Anchor | ) | WT Docket No. 17-97 |
| | ) | |

## COMMENTS OF CTIA

CTIA[1] respectfully submits these comments in response to the Notice of Inquiry ("NOI") released by the Federal Communications Commission ("FCC" or "Commission") in the above-captioned proceeding seeking input on methods to authenticate telephone calls.[2]

## I. INTRODUCTION AND SUMMARY

CTIA and its members have led multi-pronged efforts to reduce illegal robocalls, including in the industry *Robocall Strike Force*. CTIA is encouraged by progress on call authentication protocols in bodies such as ATIS, the SIP Forum and the Internet Engineering Task Force (IETF). The SHAKEN/STIR framework developed by these standard-setting bodies has received widespread acclaim and is being deployed. As protocols are developed and deployed, the Commission should continue to support the work of industry and standards bodies.

Industry supports the FCC's interest in promoting call authentication, including the implementation of a trust anchor, as one of many tools to reduce illegal robocalls. U.S. carriers

---

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st-century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] *See Call Authentication Trust Anchor*, Notice of Inquiry, WC Docket No. 17-97, FCC 17-89 (rel. July 14, 2017) ("NOI").

need confidence in the digital certificates that underlie call authentication. As Chairman Pai urged last year, the Commission should move quickly "to designate a governance authority and administrator so that the certification process envisioned by the SHAKEN/STIR framework can get underway."[3] The Commission should:

- Promote flexible governance that supports industry leadership in promoting authentication;
- Encourage but not mandate authentication solutions, and encourage industry to work out implementation issues in standards bodies; and
- Recognize that call authentication is a global problem and take a leadership role to encourage other nations to participate in call authentication efforts.

These steps will promote effective call-authentication and help address illegal robocalls, continuing long-term efforts in which industry and the FCC must work together.

## II. CTIA SUPPORTS A "HYBRID" TRUST-ANCHOR GOVERNANCE STRUCTURE, INFORMED BY INDUSTRY CONSENSUS.

CTIA supports a hybrid governance model where industry defines and operates the structure with regulatory endorsement from the FCC. This structure, as explained by ATIS, retains flexibility to respond to evolving challenges and pursue new approaches.[4] Effective call authentication requires industry leadership, so CTIA urges the Commission to look to industry to shape the roles required to operate SHAKEN/STIR.[5]

---

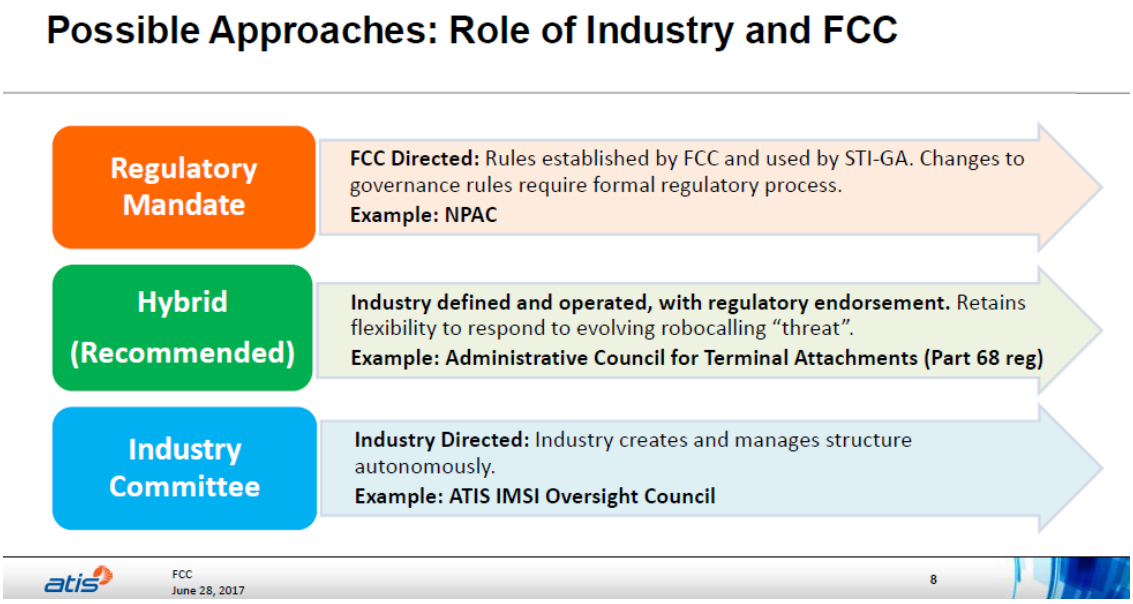
[3] Ajit Pai, Commissioner, Fed. Comm. Comm'n, Remarks at the Final Meeting of the Robocall Strike Force (Oct. 26, 2016), https://apps.fcc.gov/edocs_public/attachmatch/DOC-341999A1.pdf ("Commissioner Pai Remarks").

[4] Robocalling: Secure Telephone Identity Governance Authority (STI-GA) Proposal, *attached to* Letter from Thomas Goode, General Counsel, Alliance for Telecommunications Industry Solutions ("ATIS"), to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59 (filed June 30, 2017) ("ATIS June 30, 2017 Ex Parte").

[5] NOI ¶ 11 (identifying the roles for call authentication to be: governance authority, policy administrator, certificate authorit(ies) and service providers.).

### A. The FCC Can Be An Effective Governance Authority, And Should Rely On Standards Bodies For Implementation.

A governance authority is the domain of the national regulatory body, here the FCC. CTIA supports ATIS' hybrid model, in which the FCC has latitude to delegate supervision and management. As governance authority, the FCC would provide regulatory direction or endorsement of an approach, and then allow industry to implement that direction itself or through a separate organization or standards body.




*From ATIS June 30, ex parte filing.*[6]

An industry body is the best way to convene the various stakeholders to develop standards. Industry has technical expertise, experience developing consensus-based standards, and is on the front line dealing with robocalls. This structure ensures flexibility and speed. Illegal robocalls are an evolving threat, which makes it important to act quickly in response to

[6] ATIS June 30, 2017 Ex Parte. STI-GA is the Secure Telephone Identify Governance Authority; the NPAC is the Number Portability Administration Center; and the ATIS IMSI Oversight Council is the International Mobile Subscriber Identity Oversight Council.

changing tactics. Third-party standards are easier to adjust than FCC rules, as standards are not subject to formal notice-and-comment processes. A regulatory approach would be slower and allow bad actors to outpace current policies.

The Administrative Council for Terminal Attachments ("ACTA"), which manages the FCC's Part 68 regulations, offers a model that could be employed for call-authentication governance. ACTA was formed through co-sponsorship and support of the Alliance for Telecommunications Industry Solutions ("ATIS") and the Telecommunications Industry Association ("TIA"). It is an:

> open organization established to: (1) adopt technical criteria and to act as the clearing-house, publishing technical criteria for terminal equipment developed by ANSI-accredited standards development organizations; and (2) establish and maintain a registration database of equipment approved as compliant with the technical criteria. The Administrative Council will not make substantive decisions regarding the development of technical criteria.[7]

The FCC authorizes this structure and provides oversight. This could be a model for a hybrid approach to call authentication governance.

No matter how the FCC approaches governance, it should consider how its approach might affect its international counterparts and their willingness to advance similar priorities. Effective call authentication will require cooperation with international partners. How the FCC structures the governance authority likely will affect how other countries structure theirs.

### B. The Role Of Policy Administrator Can Be Identified By Working With Industry To Create A Hybrid Model, As ATIS Suggests.

Industry should help determine the policy administrator. The policy administrator "applies the rules set by the governance authority and confirms that certification authorities are

[7] Administrative Council for Terminal Attachments, https://www.part68.org/ (last visited Aug. 14, 2017).

authorized to issue certificates, and that service providers are authorized to request and receive certificates."[8] The NOI explores a variety of methodologies, including LLCs, for this role.[9] CTIA is not opposed to a single entity taking on both the governance authority and policy administrator roles, but that should be determined in consultation with industry.[10] CTIA supports the FCC, or an FCC-delegated entity, designating or assigning Policy Administrator responsibilities to an entity that has industry support. Using an LLC has worked in other contexts and could work in the call authentication context.

The NOI asks whether entities currently carrying out delegated functions have the right structure and experience to serve as policy administrator.[11] None of the existing entities or LLCs identified by the FCC are an obvious fit. CTIA does not support appointing the NANPA, the Pooling Administrator, or the LNPA as the policy administrator.[12] The NANPA manages numbers and number ranges, whereas a policy administrator will oversee service providers and call authentication methodologies – very different responsibilities. Combining these initiatives may not make sense; without additional resources and FCC oversight, it may dilute these distinct efforts. Nor does the LNPA appear to be a viable option. The NPAC database is not a complete line-level database; it only has numbers that have been ported or pooled, limiting the information it could use to authenticate calls. CTIA likewise does not see a role for the NANC in call-authentication governance.[13] The differences between numbering administration and call

---

8 NOI ¶ 11.

9 *Id.* ¶ 19-20.

10 *Id.* ¶ 18.

11 *Id.* ¶ 21.

12 *Id.* ¶¶ 21-24.

13 *Id.* ¶ 27.

authentication mean there are few, if any, synergies in the NANC having a role in this process. The Commission should look to standards bodies to determine what entities have the right structure and experience to oversee call authentication. CTIA stands ready to help the Commission with this task.

### C. CTIA Supports ATIS' Recommendations With Respect To Certification Authorities And Service Provider Requirements.

CTIA supports ATIS' recommendations that certification authorities have "sufficient certificate management expertise; and … an in-market presence (i.e. being incorporated in the U.S.)."[14] Certification authorities "issue the certificates used to sign and verify telephone calls."[15] Carriers can act as a certification authority and/or an authentication service. As for more general implementation, the multi-stakeholder process is well suited to determine criteria for certification authorities and the number of certification authorities.[16]

CTIA also supports ATIS' recommendations on service-provider requirements, such as requiring service providers to have an Operating Company Number (OCN) to sign calling-party information.[17] This is a simple definition that carriers supported at the ATIS IP-NNI (IP-based network-to-network interface) Task Force. Such simplicity outweighs any perception that provider-level certification will stymie novel uses of this system.[18] In fact, we have seen no evidence to support that perception.

---

14 *Id.* ¶ 29.

15 *Id.* ¶ 11.

16 *Id.* ¶ 32

17 *Id.* ¶ 30.

18 *Id.* ¶ 31.

## III. THE COMMISSION SHOULD PROMOTE INTERNATIONAL USE OF AUTHENTICATION SOLUTIONS.

The SHAKEN/STIR framework is the appropriate framework for call authentication, having been developed and endorsed by much of the mobile ecosystem.[19] To promote call authentication, the FCC should encourage the implementation of SHAKEN/STIR domestically and promote call authentication overseas.

The industry is in the early stages of call authentication; regulation or mandates will impose significant costs but have only marginal utility.[20] *First*, current protocols are not sufficiently established to justify mandatory adoption. The FCC must encourage flexibility and allow the standards process to run its course before considering regulation. SHAKEN/STIR was developed through a consensus process, which is ongoing. Until tools are fully developed, used, and refined, the FCC should avoid any regulatory steps that could hinder innovation.

*Second*, use of call authentication imposes costs, and not all domestic carriers are ready to adopt the SHAKEN/STIR framework at this early stage. This is especially true for small and mid-size carriers. Annual on-going costs of implementing a call authentication system can be substantial, particularly for small and mid-size operators.[21] Cost recovery for voluntary use of authentication protocols should be addressed as needed by industry consensus, but the Commission should understand that implementing a call authentication protocol like SHAKEN/STIR is costly and small or mid-size companies may struggle with it.

*Third*, a U.S. regulatory solution will have limited effect, so burdening U.S. operators with a mandate would not make sense. The NOI correctly observes that illegal robocalling and

---

19 *Id.* ¶ 17.

20 *Id.* ¶ 14.

21 *Id.* ¶ 46-47.

spoofing are global problems and that "adopting authentication frameworks in the U.S. will naturally have less effect on foreign robocalling."[22] Bad actors manipulate the system by "originating the calls outside the U.S. and routing them so they appear to be from inside the country."[23] Congress recognizes this, as evidenced by the Senate's recent passage of S. 134, the Spoofing Prevention Act of 2017. If enacted, it would amend 47 U.S.C. § 227(e)(1) to cover persons outside the U.S. that transmit misleading or inaccurate caller identification information into the U.S. Expansion is appropriate, but new U.S. legal standards may not be enough to change the behavior of overseas bad actors. As a result, even full U.S. deployment of call authentication technology will not solve the problem entirely. Call authentication requires widespread adoption to be effective. The FCC should support international efforts to implement better solutions ubiquitously, such as SHAKEN/STIR.

The U.S. should champion solutions abroad. The FCC is working with other nations, but most are not yet engaged. So far only Canada and the United Kingdom have taken an interest in robocall mitigation and the utility of the SHAKEN/STIR protocol. The 2016 Memorandum of Understanding ("MOU") on *Mutual Assistance in the Enforcement of Laws on Automated Telephone Calls and Inaccurate Caller Identification* between the FCC and the Canadian Radio-Television and Telecommunications Commission is an example of how the FCC can support call authentication globally.[24] More such MOUs are necessary, and U.S. leadership is needed to build consensus.

---

22 *Id.* ¶ 40.

23 Olga Kharif, *The New Weapons in the Fight Against 2.4 Billion Robocalls*, Bloomberg News (Aug. 31, 2016), https://www.bloomberg.com/news/articles/2016-08-31/with-pesky-robocalls-on-the-rise-tech-forces-amass-to-stop-them.

24 *MOU Between The United States Federal Communications Commission And The Canadian Radio-Television And Telecommunications Commission On Mutual Assistance In The Enforcement Of Laws On Automated Telephone Calls And Inaccurate Caller Identification*,

*Finally*, U.S. solutions may have unintended consequences that complicate robocall abatement, making it prudent for the Commission to rely on standards work and international advocacy. The use of call authentication in the U.S. without similar steps abroad may push more robocall originating points offshore, making location and enforcement more challenging. Tracking international calls is difficult and will likely rely on tracebacks with other carriers. Paradoxically then, a focus on domestic regulation to promote call authentication may make it harder to prevent and identify illegal robocalls. That does not mean that U.S. call authentication efforts should not be pursued vigorously, but it does suggest that mandates and prescriptive regulation are premature, to say the least. The FCC should remain cognizant that actions taken in the U.S. will affect the incentives of bad actors; the global ecosystem needs collaborative, flexible efforts in lieu of mandates.

## IV. OPERATIONAL AND POLICY QUESTIONS WILL BE ADDRESSED IN STANDARDS BODIES AND OTHER FORUMS.

ATIS, the SIP Forum, and the NNI Task Force are addressing implementation of call authentication. The FCC should support flexible solutions that can help abate illegal robocalls and promote rapid deployment.

### A. Standards Bodies Are Working On Implementation Issues Like Enrollment And Communication Protocols.

Prompt deployment of call authentication demands simplicity and ease of use, so the Commission should only endorse policies that further those goals. The NOI asks about implementation of call authentication frameworks, including enrollment, what entities can

Enforcement Bureau (Nov. 17, 2016), https://www.fcc.gov/document/fcc-canadian-radio-television-and-telecommunications-commission-mou.

perform authentication, and communication protocols. CTIA urges the FCC to support ongoing standards work, which will address these issues.

With respect to enrollment in the certification system, of the three models identified in the NOI,[25] CTIA supports the current, top-down structure. A top-down structure enhances security and accountability, because the policy administrator monitors certification authorities, and service providers cannot seek a certificate until they get a token from the policy administrator. Again, ease of use is key to making this work. By contrast, a bottom-up enrollment process, such as through text-message authentication (where, for example, the certification authority sends a URL over text message so the user can confirm it is the originating telephone number), is unduly complex and could create confusion. Enterprise-level certification and delegations may be workable, but industry should be left to handle associated complexities and governance challenges.

Likewise, the Commission need not grapple now with what "entities" should be able to perform call authentication. The NOI asks whether other "entities," besides large providers and third-party proxies could provide authentication services, specifically asking about the role of end user devices.[26] As IETF explains, device-level authentication is complex, so CTIA does not at this time support this approach. The FCC should promote available authentication methods and promote flexibility for innovation. As other authentication methods become viable, industry will deploy them, in coordination with the FCC and other stakeholders.

---

[25] The NOI identifies three options for enrollment of authorized numbers or providers: top-down central authority control (which the SHAKEN framework relies on), a bottom-up approach in which "a certification authority would require an entity to prove its control over a number by some sort of test," or a delegation approach, in which a certificate holder "can delegate to another party its authority to vouch for a number or set of numbers." *Id.* ¶ 34.

[26] *Id.* ¶ 35.

The Commission should support industry-developed methods for communication between service providers and certification authorities. The NOI asks about Automated Certificate Management Environment ("ACME"), the protocol that service providers will use to communicate with certification authorities.[27] The Commission suggests that because ACME is still under development, perhaps it should consider other mechanisms as interim solutions. ACME is promising and is currently being developed and worked through the industry-consensus process.[28] As part of its flexible support for industry efforts, the FCC should consider making other solutions permissible, but right now, ACME is the best option.

### B. Call Authentication Complements Other Efforts, Making It Unnecessary To Address Any Privacy And Security Issues.

Call authentication solutions like SHAKEN/STIR fit comfortably in the larger policy landscape surrounding illegal robocall abatement and the promotion of flexible solutions to protect consumers from spoofing and other harmful activity. Call authentication is one of the key elements of the work being done by the industry *Robocall Strike Force*. As Chairman Pai said last year, "spoofing is a, if not *the*, critical input that enables robocalling. Scammers and spammers using spoofing to disguise their identity, to trick consumers into answering unwanted calls, and to hide from authorities."[29] CTIA appreciates the FCC's support for creative solutions that empower industry to help consumers. Proceeding with call authentication solutions promotes other Commission priorities and the public interest.

---

27 *Id.* ¶ 36.

28 *Id.*

29 Commissioner Pai Remarks (emphasis in original).

CTIA agrees with IETF that privacy concerns are not likely to be impacted by SHAKEN/STIR or other authentication efforts.[30] To eliminate any concern from providers about sharing information to authenticate calls, the FCC should clearly and unambiguously state that industry efforts to implement SHAKEN/STIR or similar frameworks do not violate privacy principles or obligations, such as the provisions of 47 U.S.C. § 222. Risks of harm to consumers from this sort of information-sharing between providers are hard to identify, particularly when balanced against the benefits to consumers from ensuring the legitimacy of calls and helping end the leading cause of consumer complaints. The FCC should not let inchoate privacy worries undermine this effort by, for example, entertaining the concept of an authentication service acting as a "privacy service," as discussed in the NOI.[31] Stripping out some information or honoring users' request to eliminate identifying information from the call, as the Commission acknowledges, will "prevent the authentication service from vouching for the call."[32] This would undermine the purpose of call authentication.

Likewise, SHAKEN/STIR is important for security.[33] Call authentication will improve security in the ecosystem, by helping validate traffic crossing networks. As with any security solution, it could be targeted for compromise, but these risks are small and ably managed by providers, certificate authorities, and others in the ecosystem. This is why a robust governance

---

30 NOI ¶ 42.

31 *Id.* ¶ 43. Further, privacy is already incorporated in service provider networks when displayed caller ID is blocked at the originator's request, and this blocking will not be affected by SHAKEN. A call can be signed and verified under SHAKEN and show verification status (Yes/No) even if the caller invokes *67 caller ID blocking.

32 *Id.*

33 *Id.* ¶ 44.

structure managed by experienced participants is important. Industry will address any security risks from the use of authentication frameworks in their networks.

### C. The FCC Should Not Make Legacy System Challenges An Impediment To Deploying Call Authentication For Modern Networks.

This proceeding appropriately deals with the ATIS/SIP Forum proposals for authentication standards for calls using SIP-based networks. Questions about interoperability between Signaling System Number 7 (SS7) with SHAKEN/STIR[34] should not impact support for or progress on SHAKEN/STIR as an approach to address call authentication. As regulators and innovators have been urging, the global communications industry has actively deployed and continues to look ahead to IP-based voice telephony. The cable industry has been moving to SIP/VoIP. The mobile industry is evolving to VoLTE or end-to-end SIP. The private sector has heeded the consistent message to sunset the PSTN network and move to an all-IP system. Further, the cost, availability, traffic trends, and evolutionary benefits of calls over VoIP from overseas locations all favor that technology over TDM. Thus, it makes sense to focus on SIP-based networks when it comes to call spoofing and call-authentication efforts. This does not mean that industry is ignoring legacy systems, but innovation is focusing on the future. Due to limitations in the SS7 protocol and infrastructure, the SHAKEN/STIR approach does not lend itself to being extensible to SS7, nor is it intended to integrate authentication across both IP and older-TDM systems. Finally, the industry *Robocall Strike Force* considered applications of call authentication frameworks to legacy systems, but concluded such application was not feasible. [35]

---

[34] *Id.* ¶¶ 38-39, 44.

[35] According to an ATIS presentation on SHAKEN/STIR, "[e]xisting PSTN Class 5 TDM/SS7 equipment is at or near End of Life [EOL] and cannot be modified." *Mitigation Techniques for Unwanted Robocalls: Updates on ATIS and Other Key Industry Initiatives*, ATIS (Oct. 12, 2016), https://www.atis.org/01_news_events/webinar-pptslides/robocallslides_final.pdf.

## V. CONCLUSION

CTIA appreciates the Commission's support of industry efforts to help consumers avoid illegal and annoying robocalls and other spoofed calls. A call authentication trust anchor is an important step. CTIA urges the Commission to remain flexible and help industry to continue leading, in efforts like the industry *Robocall Strike Force*. The Commission should avoid mandating solutions that may be prohibitively expensive for smaller carriers, with relatively little benefit in stopping an inherently global challenge. Instead, the Commission should focus on supporting industry work and encouraging widespread adoption of call authentication protocols at home and abroad.

Respectfully submitted,

*/s/ Scott Bergmann*

Scott Bergmann
Vice President, Regulatory Affairs

Thomas C. Power
Senior Vice President, General Counsel

Melanie K. Tiano
Director, Cybersecurity and Privacy

**CTIA**
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

August 14, 2017